Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2014–2015

33 662

Wijziging van de Wet bescherming persoonsgegevens en enige andere wetten in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens alsmede uitbreiding van de bevoegdheid van het College bescherming persoonsgegevens om bij overtreding van het bepaalde bij of krachtens de Wet bescherming persoonsgegevens een bestuurlijke boete op te leggen (meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid Cbp)

C

MEMORIE VAN ANTWOORD

Ontvangen 19 mei 2015

1. Inleiding

Ik dank de leden van de vaste commissie voor Veiligheid en Justitie voor het voorlopig verslag. Graag beantwoord ik de in het voorlopig verslag gestelde vragen en ga ik, voor zover daartoe aanleiding is, op de gemaakte opmerkingen in. Deze memorie wordt mede uitgebracht namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Economische Zaken. Hopelijk zal de beantwoording bijdragen aan een spoedige verdere behandeling van dit wetsvoorstel.

Het doet mij genoegen dat de leden van de **VVD**-fractie met belangstelling hebben kennisgenomen van het wetsvoorstel. Met deze leden ben ik van mening dat dit wetsvoorstel een belangrijke bijdrage kan leveren aan het verbeteren van de informatiebeveiliging van veel organisaties die onder de Wet bescherming persoonsgegevens (hierna: Wbp) vallen, alsook aan het verbeteren van de bescherming van de persoonlijke levenssfeer van betrokkenen.
Het verheugt mij dat de leden van de **PvdA**-fractie met instemming hebben kennisgenomen van het wetsvoorstel. Zij kunnen zich vinden in de aan het Cbp geboden mogelijkheid om een bestuurlijke boete op te leggen bij het niet melden van datalekken. Ook vinden deze leden het wijs dat het opleggen van een dergelijke boete in de meeste gevallen voorafgegaan moet worden door een (bindende) aanwijzing. Zeker omdat – en hier hebben de meeste vragen betrekking op – niet geheel klip-en-klaar is wanneer een datalek aan het Cbp en/of betrokkenen moet worden gemeld en wanneer niet.

kst-33662-C
ISSN 0921 - 7371
’s-Gravenhage 2015

Het doet mij genoegen dat de leden van de **CDA**-fractie met belangstelling hebben kennisgenomen van het wetsvoorstel en dat zij het doel van de voorgestelde meldplicht en van andere meldplichten met betrekking tot datalekken of andere ernstige incidenten met betrekking tot de bedrijfsvoering, onderschrijven. Ik deel hun mening dat deze meldplicht zal bijdragen aan het vergroten van het vertrouwen van het publiek in digitale gegevensverwerking. Mocht zich immers een datalek voordoen, dan zal de betrokkene van wie de persoonsgegevens zijn gelekt, door desbetreffend bedrijf of (overheids)organisatie op de hoogte worden gesteld indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Deze meldplicht wordt neergelegd in artikel 34a, tweede lid, Wbp. Met de melding voldoet de verantwoordelijke aan zijn verplichting om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking van zijn persoonsgegevens te waarborgen. De meldplicht maakt duidelijk dat die verplichting niet ophoudt te bestaan indien de beveiliging van de persoonsgegevens is doorbroken of omzeild, dan wel geheel ontbrak. De meldplicht strekt ertoe betrokkene te informeren over het datalek, de instantie(s) waar meer informatie kan worden verkregen, en over door hem of haar zelf te treffen maatregelen om de negatieve gevolgen van de inbreuk zoveel mogelijk te beperken. Op deze wijze wordt voorkomen dat een datalek een onnodig grote impact heeft op de persoonlijke levenssfeer van de getroffen personen.

Daarnaast zal het wetsvoorstel, zoals deze leden terecht stellen, eraan kunnen bijdragen dat er lessen worden geleerd van opgetreden datalekken. Ten eerste worden bedrijven en (overheids)organisaties zelf verplicht om een overzicht bij te houden van de (potentieel) ernstige lekken die aan de toezichthouder zijn gemeld (artikel 34a, achtste lid, Wbp). Het centraal beschikbaar zijn van deze informatie zal het lerend vermogen van organisaties bevorderen. In de tweede plaats zal de toezichthouder (het College bescherming persoonsgegevens, straks: de Autoriteit persoonsgegevens) via zijn jaarverslag, richtsnoeren, of in andere publicaties (bijvoorbeeld antwoorden op veelgestelde vragen) informatie geven over hoe datalekken kunnen worden voorkomen, hoe ze kunnen worden afgehandeld en welke vormen van kennisgeving geschikt zijn om getroffen personen op de hoogte te brengen (best practices).

Ik ben het graag met de leden van de **CDA**-fractie eens, dat een geclausuleerde omschrijving van de meldplicht in verband met het toezicht en de handhaving van de meldplicht noodzakelijk is. Zonder een goede afbakening zou de handhaving van de meldplicht door het Cbp onbeheersbaar worden en de effectiviteit van de meldplicht teniet worden gedaan.

Deze leden stellen vervolgens vast dat de meldplicht, ondanks dat de titel van het wetsvoorstel anders doet vermoeden, alleen betrekking heeft op een doorbroken beveiliging. Hoewel deze leden aan deze constatering geen vraag verbinden, merk ik daarover graag het volgende op. Hoewel de ruimere aanduiding in het opschrift («meldplicht datalekken») inderdaad anders zou doen vermoeden, is de meldplicht nadrukkelijk bedoeld voor situaties waarin sprake is van een doorbreking van technische en organisatorische maatregelen die voor de beveiliging van persoonsgegevens zijn getroffen. Zoals in het nader rapport en de nota naar aanleiding van het verslag (nrs. 4 en 6) is aangegeven, mag hieraan niet de conclusie worden verbonden dat indien een verantwoordelijke in het geheel geen beveiligingsmaatregelen heeft getroffen, de meldplicht niet van toepassing is. In dit opzicht beoogt het wetsvoorstel een ruime uitleg van een «doorbroken beveiliging». Tegelijkertijd is het element van een doorbroken beveiliging van belang in de afgrenzing van de reikwijdte

van de meldplicht voor datalekken ten opzichte van andere situaties, waarin niet noodzakelijkerwijs sprake hoeft te zijn van een doorbroken beveiliging van persoonsgegevens, zoals bijvoorbeeld het schenden van een geheimhoudingsverplichting ten behoeve van het aan de kaak stellen van een misstand in een organisatie (klokkenluiden) of waarin sprake is van een aantasting van voorzieningen van algemene aard en niet van specifieke, op beveiliging van persoonsgegevens gerichte voorzieningen, zoals het geval is bij een brand die (delen van) een of meerdere bedrijfsgebouwen kan betreffen.

Ik constateer dat de leden van de **SP**-fractie met gemengde gevoelens hebben kennisgenomen van het wetsvoorstel. Zij wijzen erop dat de Tweede Kamer tien jaar geleden de motie-Gerkens/Van Dam heeft aangenomen die de regering opriep tot het instellen van een meldplicht (Kamerstukken II 2005/06, 26 671, nr. 20). Het heeft in hun ogen lang geduurd, veel te lang, voordat deze motie is omgezet in een wetsvoorstel. Dat het wetsvoorstel er nu daadwerkelijk is, verheugt deze leden dan ook zeker. Zij zien het wetsvoorstel als een stap vooruit. Zij wijzen er bovendien op dat de maatregel kan rekenen op een groot draagvlak, zo getuige ook de behandeling in de Tweede Kamer.

Met deze leden ben ik verheugd dat het wetsvoorstel er nu is en op een groot draagvlak kan rekenen. Wat de door deze leden aangehaalde voorgeschiedenis betreft, merk ik op dat de met algemene stemmen aanvaarde motie-Gerkens/Van Dam in 2005 werd ingediend bij de plenaire behandeling van het wetsvoorstel inzake de wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II). In dat debat stonden ontwikkelingen op het gebied van informatietechnologie en bestrijding van cybercriminaliteit centraal. In de eerdere versie van de motie (nr. 18) overwogen de indieners dat burgers en bedrijven het recht hebben te weten wat er gebeurt met persoonlijke gegevens die zij digitaal aan anderen hebben gegeven. In verband daarmee werd de regering verzocht om een voorstel uit te werken dat zou leiden tot de verplichting van bedrijven, overheden en andere organisaties om burgers en bedrijven te informeren dat hun gegevens ontvreemd zijn, of dat de systemen van de organisatie gehackt zijn. De oorspronkelijke motie vroeg om voor 1 juni 2006 met een dergelijk voorstel naar de Kamer te komen. In het debat daarover, op 13 september 2005, stelde de toenmalige Minister van Justitie dat het informeren van de klant na een aanval van hackers een kwestie is die door het privaatrecht wordt beheerst en zich om die reden niet leent voor een regeling in het strafrecht. Daarop hebben de indieners de motie gewijzigd. In de gewijzigde motie (nr. 20) werd de regering verzocht om in kaart te brengen wat de positieve en negatieve gevolgen zouden kunnen zijn van het instellen van een meldplicht om burgers op de hoogte te brengen wanneer hun gegevens ontvreemd zijn, daarmee meenemend de ervaring die met een dergelijke wet zijn opgedaan in de Verenigde Staten.

In de brief van 8 april 2009 aan de Voorzitter van de Tweede Kamer der Staten-Generaal (Kamerstukken II 2008/09, 26 643, nr. 138) hebben de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Economische Zaken verslag gedaan van de uitkomsten van het onderzoek naar de ervaringen met een dergelijke (al dan niet vrijwillige) meldplicht in een aantal andere, Europese en niet-Europese, landen en naar de mogelijke vormgeving van een meldplicht bij verlies van privacygevoelige gegevens in Nederland.
Uit het onderzoek bleek onder andere dat er onder de respondenten in het algemeen veel belang werd gehecht aan een in EU-verband geharmoniseerde meldplicht. Door de invoering van een EU-brede meldplicht

zouden bedrijven gestimuleerd worden om de beveiliging van privacygevoelige gegevens beter te regelen en op een gezonde wijze te concurreren. Inmiddels was op EU-niveau een (sectorale) meldplicht datalekken voor aanbieders van openbare elektronische communicatiediensten in voorbereiding en gingen stemmen op deze te verbreden naar alle diensten van de informatiemaatschappij (zoals webwinkels, banken etc.). Omdat een goede privacybescherming van cruciaal belang is voor het vertrouwen in diensten die via internet worden aangeboden gaf het kabinet in de bovenbedoelde brief aan dit voorstel te ondersteunen en, na afronding van de besluitvorming op Europees niveau (herziening e-privacyrichtlijn), over te gaan tot de (nationale) invoering van een (brede) meldplicht ingeval van verlies van persoonsgegevens uit informatiesystemen. Het is mede hierdoor dat de invoering van een dergelijke meldplicht voor datalekken in het regeerakkoord van het kabinet-Rutte I van 30 september 2010 is opgenomen. In vervolg hierop heeft eind 2011 de (internet)consultatie plaatsgevonden over een wetsvoorstel tot wijziging van de Wbp dat twee maatregelen bevatte, te weten de meldplicht datalekken en een verruiming van het gebruik van camerabeelden van strafbare feiten ten behoeve van de ondersteuning van de rechtshandhaving. Naar aanleiding van het advies van de Afdeling advisering van de Raad van State van 14 september 2012 is medio 2013 alleen de meldplicht voor datalekken bij de Tweede Kamer ingediend. Overeenkomstig het regeerakkoord van het kabinet-Rutte II van 29 oktober 2012 is het wetsvoorstel bij tweede nota van wijziging aangevuld met een regeling voor de uitbreiding van de bestuurlijke boetebevoegdheid van het College bescherming persoonsgegevens (hierna: Cbp). Daarnaast heeft de Minister van Veiligheid en Justitie onlangs, samen met de Minister van Binnenlandse Zaken en Koninkrijksrelaties, een nieuwe (internet)consultatie gestart met een wetsvoorstel tot wijziging van de Wbp met het oog op de verwerking van camerabeelden door bedrijven en particulieren ter ondersteuning van de opsporing.
Terugkijkend op deze ontwikkelingen meen ik dat de motie-Gerkens/Van Dam een belangrijke katalysator voor de meldplicht datalekken is geweest, maar dat het zoeken naar een goede vormgeving van een wettelijke meldplicht, in samenhang met andere wetgevingsvoornemens, geruime tijd in beslag heeft genomen.

Het stemt mij tevreden dat de leden van **SP**-fractie opmerken dat de overheid met dit wetsvoorstel het duidelijke signaal afgeeft dat persoonsgegevens goed beveiligd dienen te worden. Maakt men hier geen serieus werk van en gaat er iets mis, dan kan het Cbp stevige boetes uitdelen. Zij merken voorts op, tot mijn genoegen, dat de door de Tweede Kamer aangenomen amendementen het wetsvoorstel verbeteren door de mogelijkheden van het Cbp verder te versterken. Tegelijkertijd vragen de leden van de **SP**-fractie zich af of dit wetsvoorstel uiteindelijk de positie van de consument zal verbeteren. Vooral op dit punt willen deze leden een aantal vragen stellen en opmerkingen maken. De leden van de fractie van **GroenLinks** sluiten zich daarbij aan. In het vervolg van deze memorie zal ik de vragen van de leden van deze fracties beantwoorden.

Ik constateer dat de leden van de **D66**-fractie met belangstelling hebben kennisgenomen van het wetsvoorstel. Zij merken op dat het wetsvoorstel onder meer een meldplicht invoert bij een inbreuk op beveiliging van persoonsgegevens en het Cbp meer bevoegdheden geeft om bij die inbreuk bestuurlijk op te treden door de bestuurlijke boete in te voeren. In paragraaf 5 zal ik de vragen van deze leden beantwoorden.

2. Strekking van het wetsvoorstel

De leden van de **SP**-fractie en de **GroenLinks**-fractie merken op dat de indieners van de motie-Gerkens/Van Dam een bredere meldplicht voor ogen hadden dan nu wordt voorgesteld. De consument zou volgens hen altijd op de hoogte moeten worden gesteld als er een inbreuk heeft plaatsgevonden. Zij constateren vervolgens dat de regering en de Europese instellingen ervoor hebben gekozen dit niet te doen omdat dit dan zoveel meldingen zou genereren dat het effect van de meldplicht teniet zou worden gedaan. De leden van deze fracties beamen dit, wanneer de melder altijd melding zou moeten doen bij het Cbp. Maar deze leden zijn van mening dat een ieder het recht heeft om te weten of zijn of haar gegevens wellicht bij iemand gestolen kunnen zijn. Dat is in hun ogen nodig om maatregelen te kunnen treffen om te voorkomen dat met de gegevens onrechtmatige handelingen zouden kunnen worden verricht.

Zoals de leden van de **SP**-fractie en de **GroenLinks**-fractie al opmerken, zou een zo vergaande meldplicht aan consumenten zijn doel voorbij schieten. In het wetsvoorstel, maar bijvoorbeeld ook in artikel 11.3a van de Telecommunicatiewet, waarmee de gewijzigde e-privacyrichtlijn is geïmplementeerd, is de melding aan de door het datalek getroffen persoon nadrukkelijk beperkt tot gevallen waarin de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene. Juist om die reden wordt de verantwoordelijke verplicht om aanbevelingen aan de getroffen persoon te doen om de ongunstige gevolgen voor diens persoonlijke levenssfeer zoveel mogelijk te beperken (artikel 34a lid 3). Als ongunstige gevolgen voor de persoonlijke levenssfeer niet te duchten zijn, bijvoorbeeld wanneer verloren of gestolen gegevens adequaat versleuteld zijn, dan is het informeren van de consument niet nodig en is er geen reden om aan bedrijven en (overheids)organisaties een dergelijke verplichting op te leggen.

De aan het woord zijnde leden merken vervolgens op dat de bewustwording ten aanzien van het belang van een goede beveiliging van persoonsgegevens onder ondernemers en consumenten nog te wensen overlaat. Zij illustreren hun opmerkingen door erop te wijzen dat er in Nederland vele webwinkels zijn die massa's gegevens vragen zonder een beveiligde verbinding te gebruiken. Zij vermelden dat toen de vereniging HCC in 2013 een meldpunt hierover opende, er zelfs meldingen binnen kwamen van onbeveiligde pagina's van een grote pensioenuitvoerder die de complete overdrachtsgegevens van verzekerden en hun partners over een niet-beveiligde lijn liet invullen. Kinderdagverblijven hadden online inschrijfformulieren en zorgverzekeraars hadden contactformulieren met burgerservicenummers die niet beveiligd waren. HCC nam iedere keer contact op met het bedrijf met het verzoek de pagina's te beveiligen. Daaruit bleek dat veel ondernemers gewoonweg niet wisten dat deze beveiligd dienen te zijn. Zo gaven veel ondernemers aan dat ze hun website door een professioneel bedrijf hadden laten maken en dat «het dus wel goed zou zitten» of men reageerde met de opmerking dat naam, adres, geboortedatum en telefoonnummer geen persoonsgegevens zijn. Bewustwording op dit gebied bij deze ondernemers is nog heel ver te zoeken. De consument wordt daar, in de ogen van deze leden, de dupe van. Zijn of haar gegevens zijn heel eenvoudig te achterhalen. Helaas is de consument zelf zich daar ook te weinig van bewust. Anders zou deze er vaker voor kiezen om de gegevens niet in te vullen en op zoek te gaan naar een andere aanbieder. Concreet vragen deze leden wat de regering gaat doen om de bewustwording op dit gebied te verhogen.

De leden van de **SP**-fractie en **GroenLinks**-fractie snijden hier een belangrijk thema aan. Een ondermaatse beveiliging van persoonsgegevens vergroot het risico op een datalek. Daarom zijn bewustwording van het belang van een goede informatiebeveiliging en het delen van kennis cruciaal. De regering trekt zich dit zeker aan. Zo werkt de overheid op tal van manieren samen met private partners en maatschappelijke organisaties, enerzijds om het gebruik van ICT in de Nederlandse samenleving te versterken maar anderzijds ook om de weerbaarheid van de Nederlandse samenleving in het digitale domein en de bewustwording over een veilig internetgebruik te vergroten. Bij het stimuleren van het veilig gebruik van internet valt te wijzen op de activiteiten van het ECP, het platform voor de Informatiesamenleving, met onder andere het programma en de websites Veiliginternetten, Digivaardigdigiveilig en Alert Online. De websites Veiliginternetten en Alert Online bevatten tal van praktische adviezen en tips over hoe bedrijven en burgers op een veilige manier online diensten kunnen aanbieden en afnemen. Verder wordt aandacht besteed aan het belang van transparantie met betrekking tot de privacy van consumenten. Op deze websites zijn ook doorverwijzingen naar websites van andere relevante organisaties te vinden, bijv. de Consumentenbond en keurmerkorganisaties zoals Thuiswinkel.org. Verder wijs ik op de jaarlijkse publiekscampagne van Alert Online (26 oktober tot en met 6 november 2015). Ook banken zijn volop actief bij de voorlichting aan en bewustwording van klanten over de risico's van internetbankieren en over beveiligingsmaatregelen.

Als het om online veiligheid gaat, valt in het bijzonder ook te wijzen op de rol van het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid en Justitie. In 2012 publiceerde het NCSC de ICT-beveiligingsrichtlijnen voor webapplicaties, welke een leidraad bieden voor het veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur. De door deze leden genoemde kinderdagverblijven, pensioenuitvoerders en internetondernemers doen er goed aan van deze richtlijnen gebruik te maken, ook bij aan- en uitbesteding van opdrachten aan andere partijen. Ten slotte wil ik graag wijzen op de activiteiten van het Cbp. Naast zijn activiteiten in het kader van toezicht en handhaving van de Wbp, bevordert het Cbp de naleving van de Wbp via gesprekken met brancheverenigingen (bijv. Nederland ICT) en andere belanghebbenden. Met de in 2013 gepubliceerde richtsnoeren voor de beveiliging van persoonsgegevens heeft het Cbp duidelijk gemaakt wat het op het vlak van technische en organisatorische beveiligingsmaatregelen van persoonsgegevens van bedrijven en (overheids)organisaties verwacht, ter bescherming van de persoonlijke levenssfeer van klanten en burgers.

De leden van de **SP**-fractie en de **GroenLinks**-fractie merken op dat zelfs goedwillende ondernemers, die maatregelen treffen, gehackt kunnen worden. Zij zijn van mening dat een boete dan niet het meest belangrijke is, maar het informeren van de betrokkenen wel.
Ik ben het volmondig met deze leden eens, dat het inlichten van betrokkenen belangrijk is als een ondernemer is gehackt en de aard van de gestolen persoonsgegevens van dien aard is dat misbruik moet worden gevreesd. Of in deze situatie aan de ondernemer een bestuurlijke boete kan worden opgelegd, is een geheel andere vraag. Indien de ondernemer de door hem verwerkte persoonsgegevens adequaat heeft beveiligd, zie ik geen grond voor het opleggen van een bestuurlijke boete door het Cbp. Zoals onder andere in de nota naar aanleiding van het verslag (nr. 6) is opgemerkt, kan een datalek zich ook voordoen als sprake is van een adequate beveiliging. Dat wil zeggen dat de beveiligingsmaatregelen rekening houden met de stand van de techniek en de kosten van de tenuitvoerlegging, gelet op de risico's die de verwerking en de aard van

de te beschermen persoonsgegevens met zich brengen. Een boete voor overtreding van de beveiligingsverplichting van artikel 13 Wbp is dan niet aan de orde. Zou de ondernemer nalaten om de betrokkene in te lichten terwijl er wel ongunstige gevolgen voor diens persoonlijke levenssfeer zijn te duchten, dan kan het Cbp uiteraard wel een bestuurlijke boete opleggen.

De leden van de **SP**-fractie en de **GroenLinks**-fractie willen de volgende situatie aan de regering voorleggen om het belang van het inlichten van de betrokkene te illustreren. Afgelopen zomer werd er ruim een miljard gegevens buitgemaakt op internet. In oktober bleek dat hier een ruim miljoen e-mailadressen en inloggegevens, inclusief wachtwoorden, van Nederlanders tussen zaten. Het Nationaal Cyber Security Centrum (NCSC), dat onderdeel is van het Ministerie van Veiligheid en Justitie, heeft vervolgens contact gehad met de internetproviders die de betreffende Nederlandse e-mailadressen hadden uitgegeven. De providers konden getroffen gebruikers informeren dat ze slachtoffer waren geweest van de hack. «Mensen in het bezit van een e-mailadres eindigend op.nl die geen bericht van hun provider ontvangen, kunnen er over het algemeen van uitgaan dat hun e-mailadres geen onderdeel is van deze dataset», schreef het NCSC. Hoe de providers hiermee omgingen, was wisselend. Via de media berichtte de provider XS4all dat men via een tool op hun website kon zien of een e-mailadres erbij betrokken was. Als dat het geval was, was het advies om alle wachtwoorden op websites te wijzigen.

Vandaag de dag hebben mensen echter ontelbare wachtwoorden op ontelbare websites. Het is ondoenlijk om die allemaal te wijzigen, laat staan om te weten welke sites het allemaal zijn. Sommige zijn van jaren geleden, sommige hebben wel betaalgegevens, andere niet. Soms is het een inschrijving op een nieuwsbrief. Kortom, al zou men op alle websites het wachtwoord wijzigen, dan weet men nog niet of dit gehackte websites betreffen. Het NCSC zou hebben aangegeven dat ze de namen van de websites niet wil geven in verband met reputatieschade, aldus deze leden. Een betrokkene moet dus maar hopen dat de website hem of haar waarschuwt, maar de website hoeft dat niet te doen. Resultaat is dat er niets gebeurt. Dat is naar de stellige overtuiging van de leden van de **SP**-fractie en de **GroenLinks**-fractie precies waar het probleem zit en ook blijft.
Is de regering het met deze leden eens dat hiermee het grootste probleem van datalekken nog niet ondervangen is? Wetende dat geen enkele website ooit honderd procent veilig kan zijn, is dan de angst voor reputatieschade niet onterecht, en sterker nog, is de bescherming van de goede naam niet in strijd met de bescherming van de privacy en veiligheid op internet?

Graag reageer ik op de vragen van de leden van de **SP**-fractie en **GroenLinks**-fractie naar aanleiding van de omvangrijke diefstal van inloggegevens op het internet in de zomer van 2014. De gestolen gegevens kwamen vervolgens in handen van een derde partij, het Amerikaanse bedrijf Hold Security. Het NCSC heeft bij Hold Security alleen de voor de response-acties benodigde en specifiek voor Nederland relevante gegevens opgevraagd. Het NCSC heeft van Hold Security een tweetal datasets ontvangen. Een dataset van circa 5600 – mogelijk nog – kwetsbare websites binnen het.nl-domein en een dataset van circa 1,3 miljoen emailadressen die eindigen op.nl.
Zoals deze leden aangeven, zijn de eigenaren van de e-mailadressen via hun providers voor het overgrote deel bereikt. Ook werden alle eigenaren van getroffen websites via partner SIDN (Stichting Domeinregistratie Nederland) bereikt. Eigenaren kregen op deze manier de tijd om, indien nodig, de aanwezige kwetsbaarheid op hun website te verhelpen. SIDN

vroeg domeineigenaren daarnaast om hun gebruikers op gepaste wijze te informeren. Vanuit het NCSC is de keuze gemaakt om in aanvulling daarop niet ook de lijst met domeinnamen te publiceren om schade als gevolg daarvan zoveel mogelijk te beperken. Te dien aanzien is door het NCSC een – legitieme – afweging gemaakt tussen enerzijds het privacybelang van de getroffen personen en anderzijds het belang om schade voor de betrokken domeineigenaren zoals toegenomen kwetsbaarheid voor verdere aanvallen bij openbaarmaking, te voorkomen. Daarbij heeft laatstgenoemd belang zwaarder gewogen. Anders dan deze leden stellen, ging het bij deze afweging niet zozeer om de bescherming van de goede naam en reputatie van de betrokken domeineigenaren, maar veeleer om de vrees dat een openbare publicatie door het NCSC de schade voor domeineigenaren, en mogelijk daardoor ook voor betrokken personen, eerder zou vergroten dan beperken. Deze leden merken ook terecht op dat een honderd procent veilige website niet bestaat. Daarom is het van groot belang dat partijen passende maatregelen (blijven) treffen om gegevens, en in het bijzonder persoonsgegevens, te beveiligen. In de brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal van 13 oktober 2014 inzake de Hold-casus is door de Minister van Veiligheid en Justitie toegezegd dat voorts zal worden verkend hoe de ervaringen van deze casus kunnen worden geborgd in een te ontwikkelen structurele voorziening met de daarbij behorende waarborgen (Kamerstukken II 2014/15, 26 643, nr. 328).
Tegelijkertijd meent de regering dat het onderhavige wetsvoorstel met een meldplicht bij datalekken, een belangrijke verbetering voor de gebruikers van een website gaat brengen. Op grond van het voorgestelde artikel 34a Wbp, zullen de eigenaren van een website, wanneer zij aangaande hun website, al dan niet door tussenkomst van het NCSC van een diefstal van inloggegevens op de hoogte raken, in elk geval het Cbp moeten informeren en daarnaast ook de getroffen personen, indien waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van deze personen te verwachten zijn.

Over de opmerking van deze leden, dat het advies van een provider, zoals XS4All waarnaar zij verwijzen, de consument voor een vrijwel onmogelijke opgave stelt vanwege de talloze accounts op evenzovele websites merk ik op dat het in beginsel de eigen verantwoordelijkheid is van de consument om veilig te internetten om schade te voorkomen of in elk geval, bij onvermijdbare voorvallen, zoveel mogelijk te beperken. De voorlichting van het NCSC sluit hierop aan. De Hold- casus onderstreept het advies van het NCSC aan alle internetgebruikers om regelmatig wachtwoorden te wijzigen en verschillende inlognaam/wachtwoordcombinaties te gebruiken voor verschillende digitale diensten. Op die manier kunnen de nadelige effecten van verlies of diefstal van de door de consument afgestane persoonsgegevens beperkt worden. Verder wordt geadviseerd om van sterkere mogelijkheden van toegangsbeveiliging gebruik te maken. Steeds meer online diensten bieden de mogelijkheid tot het gebruik van zogenoemde tweefactor-authenticatie (ook wel tweestapsverificatie). Hierbij dient de betrokken naast het wachtwoord ook te beschikken over bijvoorbeeld een mobiele telefoon waarop bij elke sessie een nieuwe eenmalige inlogcode verschijnt.

De leden van de **SP**-fractie en de **GroenLinks**-fractie vragen of de regering het met hen eens is dat idealiter bedrijven hun klanten zelf actief informeren bij een mogelijk datalek. Op deze wijze kan de klant zelf stappen ondernemen om zijn wachtwoord te wijzigen. Is de regering het met deze leden eens dat dit zeker moet gebeuren bij ieder lek waar ook financiële gegevens zijn buitgemaakt? Zo ja, op welke wijze wil de regering zich hiervoor inzetten? De leden zouden zich kunnen voorstellen

dat een dergelijke informatieplicht eerst op basis van zelfregulering kan worden geïntroduceerd. Graag een reactie van de regering.
Ik kan de eerste vraag van deze leden bevestigend beantwoorden. De in dit wetsvoorstel voorgestelde meldplicht strekt ertoe bedrijven en (overheids)organisaties hun verantwoordelijkheid te laten nemen indien zich bij door hen verwerkte persoonsgegevens een datalek voordoet. Als hiervan waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de klant zijn te verwachten, moet deze actief worden ingelicht. Ook moet de verantwoordelijke de klant informeren over maatregelen waarmee de ongunstige gevolgen kunnen worden beperkt, zoals het wijzigen van zijn wachtwoord.

Deze leden vragen voorts of de regering hun opvatting deelt dat het informeren van de klant zeker moet gebeuren bij ieder lek waarbij financiële gegevens van de klant betrokken zijn. Ik ben met deze leden van mening dat een datalek waarbij financiële gegevens in verkeerde handen zijn gevallen nadelige gevolgen kan hebben voor de persoonlijke levenssfeer van de betrokkene. Het informeren van de betrokkene, naast uiteraard het Cbp, ligt naar mijn mening dan ook in de rede. Dit volgt uit artikel 34a, tweede lid. Echter, het tiende lid van artikel 34a, bevat een uitzondering voor financiële ondernemingen als bedoeld in het Wet op het financieel toezicht (Wft). Deze zijn uitgezonderd van de wettelijk verplichte melding aan de klanten in verband met potentieel verstrekkende consequenties van dergelijke openbare kennisgevingen in de financiële sector. Financiële ondernemingen hebben overigens de verplichting al om incidenten, waaronder ICT-incidenten, te melden aan de toezichthouders indien die incidenten een ernstig gevaar vormen voor de integere bedrijfsuitoefening. De zorgplicht van de financiële onderneming (art. 4:24a Wft) zal daarnaast waarborgen dat zij ook zonder dat dit dwingend wordt voorgeschreven haar verantwoordelijkheid jegens haar cliënten, in rechtstreeks contact met die cliënten, zal nemen. Dat doen deze ondernemingen nu al met betrekking tot incidenten onder de Wft en dat zal niet anders zijn ten aanzien van datalekken onder dit wetsvoorstel. Artikel 4:24a Wft kan zo nodig door de Autoriteit Financiële Markten worden gehandhaafd. Aan de door deze leden gesuggereerde zelfregulering bestaat mijns inziens, in het licht van het bovenstaande, geen behoefte.

3. Beleidsmatige achtergrond

3.1 Verhouding met Europese wetgevingsvoorstellen

De leden van de **VVD**-fractie zouden graag van de regering vernemen hoe het wetsvoorstel zich verhoudt tot het wetsontwerp dat onlangs in consultatie is gegaan en dat, naar zij stellen, een implementatie beoogt van de voorgestelde EU-richtlijn over netwerk- en informatiebeveiliging (COM(2013) 48) (NIB-richtlijn), die reeds in eerste lezing door het Europees parlement is aangenomen. Deze leden merken voorts op dat in het in voorbereiding zijnde wetsvoorstel ook een meldplicht datalekken is opgenomen, die weliswaar breder is maar ook betrekking kan hebben op de in het onderhavige wetsvoorstel bedoelde datalekken. Zij vragen de regering om in te gaan op de samenloop. Zij vragen zich bovendien af of het zo kan zijn dat verantwoordelijken zowel moeten melden aan het Cbp als aan de in het wetsvoorstel genoemde autoriteit.

De door deze leden genoemde NIB-richtlijn strekt tot het geven van een impuls aan het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging. De Europese Commissie wil de beveiliging van het internet en de particuliere netwerken en informatiesystemen verbeteren door de lidstaten ertoe te verplichten hun paraatheid te

verbeteren, beter met elkaar samen te werken en door vitale partijen te verplichten adequate beveiligingsmaatregelen te nemen en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren. Voorts introduceert de NIB-richtlijn een stelsel van toezicht en handhaving op deze zorgplichten en meldplicht. Met het wetsvoorstel dat in januari 2015 in de (aanvullende) internetconsultatie is gebracht (Wet gegevensverwerking en meldplicht cybersecurity), wordt geen uitvoering gegeven aan deze richtlijn. De richtlijn is immers nog niet vastgesteld. De onderhandelingen over de richtlijn zijn nog gaande. Wel heeft het Europees parlement, zoals de leden van de **VVD**-fractie vermelden, in eerste lezing een standpunt bepaald.

De meldplicht cybersecurity uit het bovengenoemde wetsvoorstel zal gaan gelden voor inbreuken op ICT-systemen in voor de samenleving vitale sectoren voor nader bij algemene maatregel van bestuur aan te wijzen aanbieders van vitale diensten en producten. Het gaat in dat wetsvoorstel om een meldplicht die ziet op een inbreuk op de veiligheid of een verlies van integriteit van een informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst van een vitale aanbieder in belangrijke mate wordt of kan worden onderbroken. De melding stelt het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid en Justitie in staat om hulp te verlenen aan de getroffen aanbieder en om andere aanbieders te waarschuwen, met als doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken. De meldplicht cybersecurity en de meldplicht datalekken dienen derhalve andere doelen en hebben elk een daarop afgestemd bereik (wettelijke omschrijving van de voor melding in aanmerking komende inbreuken en kring van normadressaten). Dat bereik kan echter ook overlappen. Dat komt omdat beide meldplichten aangrijpen bij een inbreuk op de beveiliging van informatiesystemen van een organisatie. Bij een inbreuk op de veiligheid of een verlies van integriteit van een informatiesysteem waarop de meldplicht cybersecurity ziet, hoeven niet noodzakelijkerwijs ook persoonsgegevens in het geding te zijn, bijvoorbeeld als het elektronisch informatiesysteem een fysiek proces aanstuurt. Wanneer echter óók persoonsgegevens in het geding zijn door een inbreuk op de beveiliging die onder de meldplicht cybersecurity valt, dan zal een vitale aanbieder, mits deze uiteraard als verantwoordelijke in de zin van de Wbp is aan te merken, de inbreuk zowel bij het NCSC als bij het Cbp moeten melden.

De leden van de **VVD**-fractie vragen daarnaast hoe wordt voorkomen dat een verantwoordelijke zowel een boete opgelegd kan krijgen door het Cbp als gevolg van het niet onverwijld melden als door een andere toezichthouder. Het NCSC is, anders dan het Cbp, geen instantie die met toezicht op of handhaving van wettelijke voorschriften is belast, maar een onderdeel van het Ministerie van Veiligheid en Justitie dat primair tot taak heeft om bij gemelde incidenten hulp te verlenen. Het NCSC kan dan ook geen boetes opleggen. Hoewel de onderhandelingen over de NIB-richtlijn nog gaande zijn en de uiteindelijke tekst van de richtlijn zich niet laat voorspellen, kan niet worden uitgesloten dat de meldplicht, zoals die is vervat in genoemd wetsvoorstel gegevensverwerking en meldplicht cybersecurity te zijner tijd op onderdelen zal moeten worden aangepast en aangevuld. Wat dat laatste betreft valt bijvoorbeeld te denken aan de handhaving daarvan. Ik zeg graag toe de zorgen van de **VVD**-fractie met betrekking tot een stapeling van toezichtregimes te zijner tijd bij de ontwikkelingen te betrekken. Op dit moment kan ik daar niet op vooruitlopen.

De leden van de **CDA**-fractie merken terecht op dat met het wetsvoorstel voor een belangrijk deel wordt vooruitgelopen op de totstandkoming van de Algemene verordening gegevensbescherming (COM(2012)11), die de huidige EU-privacyrichtlijn uit 1995 zal vervangen. Anders dan deze leden veronderstellen loopt het wetsvoorstel niet vooruit op de in voorbereiding zijnde richtlijn voor de bescherming van persoonsgegevens in de sectoren van politie en justitie (COM(2012)10). De voorloper van deze richtlijn is het Kaderbesluit nr. 2008/977/JBZ. Dit kaderbesluit heeft betrekking op de bescherming van persoonsgegevens bij de politiële en justitiële samenwerking tussen de bevoegde autoriteiten van de lidstaten in strafzaken. Het in voorbereiding zijnde pakket EU-regelgeving gegevensbescherming (verordening en richtlijn politie/justitie) is gebaseerd op artikel 16 VWEU dat bij het Verdrag van Lissabon is ingevoegd en een rechtsgrondslag schept voor het vaststellen van voorschriften betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede voorschriften betreffende het vrij verkeer van die gegevens.

Hoewel de onderhandelingen over deze documenten nog in volle gang zijn – de regering sprak in de nota naar aanleiding van het verslag de verwachting uit dat deze in 2015 zal tot stand komen en in werking treden – zouden de leden van de **CDA**-fractie graag vernemen welke aanpassingen met betrekking tot de onderwerpen, die in dit wetsvoorstel aan de orde zijn, naar aanleiding van deze Europese regelgeving mogen worden verwacht.
Ik kan deze leden meedelen dat de nieuwe EU-regelgeving gegevensbescherming naar de huidige verwachting niet in 2015, doch hopelijk in 2016 tot stand zal komen. Daarna is er een implementatietermijn van twee jaar om met nationale wetgeving aan de verplichtingen van de verordening en de richtlijn te voldoen en om strijdige wetgeving in te trekken. Nu de verordening het grootste deel van materiële normstelling met betrekking tot de verwerking van persoonsgegevens gaat bevatten, waaronder een meldplicht voor datalekken, en daarnaast vele tientallen bepalingen wijdt aan de opzet van de handhaving en de sanctionering, zal de Wet bescherming persoonsgegevens moeten worden ingetrokken. In plaats daarvan zal er een Uitvoeringswet Algemene verordening gegevensbescherming moeten komen waarin onder andere een onafhankelijke toezichthoudende autoriteit wordt ingesteld. Die wet zal naar verwachting ook een regeling kunnen bevatten van de bindende aanwijzing als tussenstap bij het opleggen van een bestuurlijke boete, zoals in dit wetsvoorstel wordt voorgesteld (artikel 66).
Zoals de Minister van Veiligheid van Justitie in de brief van 23 juni 2014 naar aanleiding van de evaluatie van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens (Kamerstukken II 2013/14, 33 842, nr. 2) heeft aangegeven zal de komst van de richtlijn een goed moment zijn om de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens in hun onderling verband en samenhang te herzien. Daarbij zal ook worden overwogen om ze samen te voegen tot één wet als dat dienstig zou zijn voor de noodzakelijke samenhang en afstemming.

3.2 Verhouding tot andere meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector

De leden van de **CDA**-fractie stellen het op prijs om een beknopt maar geheel geactualiseerd overzicht te krijgen van de diverse meldplichten die betrekking hebben op datalekken of andere ernstige incidenten met betrekking tot de bedrijfsvoering van bedrijven en van de overheid, die thans gelden of binnen afzienbare tijd in Europese wetgeving zullen

worden vastgesteld. Dit overzicht zou in ieder geval de na te noemen categorieën moeten bevatten: de wettelijke basis, de adressaat van de norm, de mogelijke sancties, de bevoegdheid van de toezichthouder(s) en de mogelijkheden van rechtsbescherming. Ik verwijs deze leden naar de hieronder opgenomen overzichten.

Overzicht: huidige meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector

Grondslag meldplicht	**Karakter inbreuk**	**Voor wie geldt meldplicht?**	**Melden bij**	**Rechtsbescherming tegen handhavingsbesluit ter zake van ten onrechte niet melden**	**Sanctionerende bevoegdheden van de toezichthouder c.q. bevoegde autoriteit ten aanzien van ten onrechte niet melden**
Art. 11.3a Telecommuniecatiewet (Tw)	Inbreuk in verband met persoonsgegevens als gevolg van een inbreuk op de beveiliging, bedoeld in artikel 11.3 die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de EU	Aanbieders van openbare elektronische communicatiediensten	Autoriteit Consument & Markt, degene wiens persoonsgegevens het betreft indien de inbreuk waarschijnlijk ongunstige gevolgen heeft voor diens persoonlijke levenssfeer *(Na inwerkingtreding wetsvoorstel 33662: Cbp / Autoriteit Persoonsgegevens)*	Algemene wet bestuursrecht	Last onder dwangsom en bestuurlijke boete (art. 15.2 en 15.4 Tw). Alsnog nakoming meldplicht aan betrokken personen verlangen (art. 11.3a lid 4). *(Na inwerkingtreding wetsvoorstel 33662: Cbp / Autoriteit persoonsgegevens)*
Artikel 11a.2 Tw	Inbreuken op de veiligheid of verlies van integriteit waardoor de continuïteit van openbare elektronische communicatienetwerken en -diensten in belangrijke mate werd onderbroken.	Aanbieders van openbare elektronische communicatienetwerken en -diensten	Minister van EZ / Agentschap Telecom	Algemene wet bestuursrecht	Last onder dwangsom en bestuurlijke boete (art. 15.2 en 15.4 Tw)
Artikelen 3:10 lid 3 en 4:11 lid 4 Wet financieel toezicht (Wft) Artikel 4:24a Wft, zorgplicht financiële ondernemingen	Inbreuk op Integere bedrijfsvoering	Financiële ondernemingen	De Nederlandsche Bank / Autoriteit Financiële Markten	Algemene wet bestuursrecht	Last onder dwangsom en bestuurlijke boete (art. 1:79 en 1:80 Wft)
Artikel 18:15 Tw jo. art. 2 lid 1 onder t, Besluit elektronische handtekeningen	Inbreuk op de veiligheid of een verlies van integriteit met aanzienlijke gevolgen voor de betrouwbaarheid of vertrouwelijkheid van gekwalificeerde certificaten	Aanbieders van gekwalificeerde certificaten	ACM en Minister van VenJ (Nationaal Cyber Security Centrum)	Algemene wet bestuursrecht	Last onder dwangsom en bestuurlijke boete (art. 15.2 en 15.4 Tw)

Overzicht: Toekomstige meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector

Grondslag meldplicht	**Karakter inbreuk**	**Voor wie geldt meldplicht?**	**Melden bij**	**Rechtsbescherming tegen handhavingsbesluit ter zake van ten onrechte niet melden**	**Sanctionerende bevoegdheden van de toezichthouder c.q. bevoegde autoriteit ter zake van ten onrechte niet melden**
Artikel 19 lid 2 EU-verordening 910/2014 elektronische identificatie en vertrouwensdiensten (eIDAS) *(Vervangt de meldplicht van art. 18.15 Tw jo. Besluit elektronische handtekeningen)*	Inbreuk op de veiligheid of verlies van integriteit van vertrouwensdiensten en daaraan gerelateerde persoonsgegevens	Aanbieders van vertrouwensdiensten	Bevoegde autoriteit en, waar passend, ook bij andere betrokken autoriteiten (Minister van VenJ / Nationaal Cyber Security Centrum en Cbp)	Algemene wet bestuursrecht	Afhankelijk van uitvoeringswet; art. 16 van de verordening verplicht tot doeltreffende, evenredige en afschrikwekkende sancties
Artikel 34a Wet bescherming persoonsgegevens	Inbreuk in verband met persoonsgegevens als gevolg van een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens	Verantwoordelijken in de zin van de Wbp	Cbp (Autoriteit persoonsgegevens) en betrokkene indien de inbreuk waarschijnlijk ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene	Algemene wet bestuursrecht	Last onder dwangsom Bestuurlijke boete Alsnog nakoming meldplicht aan betrokken personen verlangen (art. 34a lid 7 Wbp)
Artikel 7 lid 2 wijzigingsprotocol Verdrag tot bescherming van persoonsgegevens (Raad van Europa)	Inbreuk in verband met persoonsgegevens	Alle verantwoordelijken voor verwerking van persoonsgegevens in de private en publieke sector	In elk geval bij de toezichthoudende autoriteit voorzover de inbreuk ernstige gevolgen heeft voor de rechten en fundamentele vrijheden van betrokkenen en voorzover geen noodzaak bestaat om een uitzondering of beperking hierop aan te brengen	Algemene wet bestuursrecht	Afhankelijk van nationale uitvoeringswetgeving
Artikelen 31 en 32 Algemene EU-verordening gegevensbescherming (Commissievoorstel)	Een inbreuk in verband met persoonsgegevens als gevolg van een doorbreking van organisatorische en/of technische beveiliging van persoonsgegevens	Verantwoordelijken in de zin van de verordening	Cbp (Autoriteit persoonsgegevens) en betrokkene indien de inbreuk waarschijnlijk negatieve gevolgen heeft voor de bescherming van de persoonsgegevens of de privacy van de betrokkene	Algemene wet bestuursrecht	Art. 79 bevat bevoegdheid voor toezichthouder om bestuurlijke boetes en waarschuwingen op te leggen bij niet naleving meldplicht. Alsnog nakoming meldplicht aan betrokken personen verlangen (art. 32 lid 4)

Grondslag meldplicht	Karakter inbreuk	Voor wie geldt meldplicht?	Melden bij	Rechtsbescherming tegen handhavingsbesluit ter zake van ten onrechte niet melden	Sanctionerende bevoegdheden van de toezichthouder c.q. bevoegde autoriteit ter zake van ten onrechte niet melden
Artikelen 28 en 29 EU Richtlijn gegevensbescherming in sectoren politie en justitie (Commissievoorstel)	Een inbreuk in verband met persoonsgegevens als gevolg van een doorbreking van organisatorische en/of technische beveiliging van persoonsgegevens	Bevoegde autoriteiten: elke overheidsinstantie die bevoegd is ten aanzien van de voorkoming, het onderzoek, de opsporing of vervolging van strafbare feiten of de tenuitvoerlegging van strafbare feiten	Toezichthoudende autoriteit (Cbp) en betrokkene personen indien de inbreuk waarschijnlijk negatieve gevolgen heeft voor de bescherming van de persoonsgegevens of de persoonlijke levenssfeer van de betrokkene en voorzover geen noodzaak bestaat om in een uitzondering of beperking op de mededeling aan betrokkene te voorzien	Algemene wet bestuursrecht	afhankelijk van implementatiewet; artikel 55 van de concept-richtlijn verplicht tot doeltreffende, evenredige en afschrikwekkende sancties
Artikel 6 Wet gegevens-verwerking en meldplicht cybersecurity	Een inbreuk op de veiligheid of een verlies van integriteit van een informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een product of dienst in belangrijke mate wordt of kan worden onderbroken	Aangewezen aanbieders in vitale sectoren en (rijks)overheid voor aangewezen producten of diensten	Minister van VenJ / Nationaal Cyber Security Centrum (NCSC)	Geen (de meldplicht heeft een vrijwillig karakter)	Geen
Artikel 14 lid 2 Netwerk- en informatiebeveiligingsrichtlijn (Commissievoorstel)	Incidenten met een aanzienlijke impact op de beveiliging van de verleende kerndiensten	Openbaar bestuur en aangewezen marktdeelnemers	Bevoegde Autoriteit	Algemene wet bestuursrecht	afhankelijk van implementatiewet; de concept-richtlijn verplicht tot doeltreffende, evenredige en afschrikwekkende sancties

4. Algemene aspecten van de meldplicht

In het voorgestelde artikel 34a, vijfde lid, wordt bepaald dat de kennisgeving aan betrokkenen van datalekken op zodanige wijze wordt gedaan dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd. De leden van de **VVD**-fractie vragen de regering om voorbeelden te geven wanneer wel en wanneer niet sprake is van zo'n behoorlijke en zorgvuldige informatievoorziening. Ook vernemen zij graag of de verantwoordelijke, als sprake is van tienduizenden of meer betrokkenen, kan volstaan met een algemene kennisgeving in verschillende media. Of moeten ook dan alle betrokkenen individueel worden geïnformeerd?
Het tweede lid van artikel 34a bevat een inspanningsverplichting voor de verantwoordelijke om de getroffen personen (zoals klanten, burgers of medewerkers) van het datalek op de hoogte te stellen. Het vijfde lid van artikel 34a geeft als algemene norm voor de wijze waarop de betrokkenen moeten worden geïnformeerd dat een behoorlijke en zorgvuldige informatievoorziening is gewaarborgd. Datzelfde lid geeft aan dat voor de beoordeling of daarvan in concrete gevallen sprake is, rekening moet worden gehouden met de aard van de inbreuk, de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens, de

kring van betrokkenen en de kosten van tenuitvoerlegging. In veruit de meeste gevallen zal de verantwoordelijke over contactgegevens van de betrokkenen beschikken en kan betrokkene individueel worden geïnformeerd. Bij meer omvangrijke incidenten kan ook een combinatie van algemene en individuele informatievoorziening geschikt zijn, zoals een mededeling op de website van het bedrijf of de (overheids)organisatie, een individuele e-mail aan getroffen klanten of burgers en het instellen van een centraal contactpunt (e-mail en telefoonnummer). Het belangrijkste is, dat zoveel mogelijk betrokkenen worden bereikt en dat zij worden geïnformeerd over de door hem of haar zelf te treffen maatregelen om de gevolgen voor de persoonlijke levenssfeer zoveel mogelijk te beperken (vijfde lid). Met enkel een bericht in de media wordt dat doel naar mijn oordeel niet bereikt.[1]

Op grond van het achtste lid van artikel 34a is de verantwoordelijke verplicht om een overzicht bij te houden van iedere inbreuk die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Dient de verantwoordelijke een dergelijk overzicht ook openbaar te maken? En hoe lang dient een dergelijk overzicht bewaard te blijven? De leden van de **VVD**-fractie verzoeken de regering op deze vragen te reageren.
Het achtste lid van artikel 34a is het spiegelbeeld van het eerste lid waarin de meldplicht aan het Cbp is geregeld. Ingevolge het achtste lid moeten bepaalde gegevens van de melding aan het Cbp intern binnen het bedrijf of (overheids)organisatie worden geadministreerd, zodat daarvan een overzicht ontstaat. Het betreft de feiten en gegevens omtrent de aard van de inbreuk alsmede de tekst van de kennisgeving aan de betrokkene. Het wetsvoorstel bevat geen verplichting om het overzicht openbaar te maken en ook geen verplichte bewaartermijn, kan ik deze leden antwoorden. Het is aan het desbetreffende bedrijf of de (overheids)organisatie zelf om te bepalen hoe lang het overzicht bewaard blijft, voor welke doeleinden, en in welke vorm.

Het Cbp zal de meldingen vertrouwelijk behandelen, zo wordt in de memorie van toelichting aangegeven. Het Cbp is een zelfstandig bestuursorgaan en valt als zodanig onder de Wet openbaarheid van bestuur (Wob). Dit kan ondernemingen in een spagaat brengen. Melden zij een hack wel bij het Cbp, dan lopen zij mogelijk schade. Melden zij niet, dan krijgen ze mogelijk een boete opgelegd door het Cbp. Welke waarborgen biedt de Wob op dit punt, zo willen de leden van de **VVD**-fractie van de regering weten.
In de memorie van toelichting heeft de regering gewezen op het belang dat het Cbp, als onafhankelijke toezichthouder, met de bij de melding verstrekte gegevens in staat wordt gesteld om zich een beeld te vormen van het datalek en een oordeel te kunnen geven over getroffen maatregelen en de kennisgeving aan de betrokkene. Het Cbp moet zo nodig ook vertrouwelijk met de verantwoordelijke kunnen overleggen. Tegelijkertijd is er een algemeen belang van openbaarheid van overheidsinformatie, zoals belichaamd in de Wet openbaarheid van bestuur (Wob), die ook voor het Cbp geldt. Ondernemingen zouden volgens de leden van de VVD-fractie bevreesd zijn dat de bij de melding aan het Cbp verstrekte gegevens door het Cbp actief dan wel passief (Wob-verzoek) openbaar worden gemaakt. Dit zou tot schade aan reputatie of concurrentiepositie van de betrokken onderneming kunnen leiden.
Naar het oordeel van de regering hoeven ondernemingen niet voor zulke effecten te vrezen. De Wob biedt een goed niveau van bescherming van de verstrekte informatie. Ik wijs op de in de Wob opgenomen uitzonde-

[1] Zie voor de telecomsector een uitwerking hiervan in Verordening (EU) nr. 611/2013 van de Commissie van 24 juni 2013, PbEU L173/2, in werking getreden op 25 augustus 2013.

ringsgronden die stellen dat openbaarmaking van informatie achterwege blijft voor zover het vertrouwelijk aan de overheid meegedeelde bedrijfs- en fabricagegegevens betreft (artikel 10, eerste lid, onder c) en voor zover het belang van openbaarmaking niet opweegt tegen het belang om onevenredige benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden te voorkomen (artikel 10, tweede lid, onder g).
Voor de volledigheid wijs ik er op dat ook andere weigeringsgronden van de Wob bij de meldplicht datalekken van belang kunnen zijn, zoals de veiligheid van de staat (artikel 10, eerste lid, onder b), het belang van opsporing en vervolging (artikel 10, tweede lid, onder c), het belang van inspectie, controle en toezicht door bestuursorganen (artikel 10, tweede lid, onder d) en de eerbiediging van de persoonlijke levenssfeer (artikel 10, eerste lid, onder d, en tweede lid, onder e).
Van een spagaat waarover deze leden spreken, is mijns inziens dan ook geen sprake. Ondernemingen hebben geen enkele reden om melding van een datalek aan het Cbp achterwege te laten. Doen zij dat wel, dan lopen ze inderdaad het risico een boete te krijgen. De meldplicht draagt bij aan het vertrouwen in de informatiemaatschappij hetgeen van groot belang is voor onze economie.

Als het gaat om de vraag hoe de meldplicht op zinvolle wijze kan worden beperkt, verwijst de regering naar de regelgeving in Duitsland en Oostenrijk waar een veel specifiekere omschrijving wordt gegeven van de datalekken die in aanmerking komen voor melding dan in het huidige wetsvoorstel wordt gehanteerd. Is de regering met de leden van de **PvdA**-fractie van mening dat de gekozen omschrijving – aanzienlijke kans op ernstig nadelige gevolgen – niet eenduidig is en voor organisaties problemen kan opleveren bij het beoordelen of zij een datalek moeten melden of niet?

De regering heeft inderdaad verwezen naar de regelgeving in Duitsland en Oostenrijk. Beide landen hebben, elk op hun eigen wijze, de meldplicht enigszins ingeperkt zodat niet elk denkbaar datalek onder de meldplicht valt. De recente Duitse wet (§42a van het Bundesdatenschutzgesetz) beperkt de meldplicht tot voorvallen met bepaalde categorieën gegevens, zoals bijzondere persoonsgegevens, persoonsgegevens die worden beschermd met een specifiek beroepsgeheim, zoals het medisch of notarieel beroepsgeheim, strafrechtelijke persoonsgegevens en persoonsgegevens met betrekking tot bankrekeningen en creditcards. In de Oostenrijkse wet wordt de meldplicht beperkt tot een algemene categorie van relatief zware gevallen (§24 (2a) van het Datenschutzgesetz 2000).

Dat die regelingen een veel specifiekere omschrijving geven van datalekken die voor melding in aanmerking komen dan de omschrijving die in het voorliggende wetsvoorstel wordt gehanteerd, zoals de leden van de **PvdA**-fractie stellen, kan ik niet onderschrijven. Ook de buitenlandse regelingen zullen afbakeningsvragen kennen en kunnen ruim of minder ruim worden uitgelegd. De in het voorliggende wetsvoorstel gehanteerde omschrijving is naar mijn mening eveneens voldoende afgebakend, zij het op een andere manier dan in Duitsland en Oostenrijk. Een meldingsplichtig datalek wordt in het wetsvoorstel als volgt omschreven: een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Bij deze omschrijving staat de ernst van de (potentiële) gevolgen van het datalek centraal. Bij de beoordeling van de impact van het datalek zijn van belang:
- de aard en de omvang van het datalek;
- de aard van de gelekte persoonsgegevens;
- de mate waarin technische beschermingsmaatregelen zijn getroffen;

- de gevolgen voor de persoonlijke levenssfeer van de getroffen personen.

In het wetsvoorstel is voor een benadering gekozen waarvan wordt verwacht dat alle normadressaten van de Wbp (van zzp'er tot multinational) ermee uit de voeten kunnen. Elke verantwoordelijke zal voor zijn eigen verwerkingen van persoonsgegevens en die waarvoor hij een bewerker inschakelt kunnen nagaan welke risico's met de verwerking zijn gemoeid en wat de gevolgen van een datalek kunnen zijn. Deze analyses kunnen de input vormen voor een beleid binnen de organisatie met betrekking tot de afhandeling van een datalek. Het Cbp zal de te maken afwegingen ondersteunen door het opstellen van richtsnoeren (beleidsregels), zodat bedrijven en (overheids)organisaties een duidelijk beeld hebben, wanneer ze een datalek moeten melden en wanneer dat niet hoeft. De meldplicht doet uiteraard niet af aan de algemene beveiligingsverplichting van artikel 13 Wbp. Bedrijven en organisaties die in een goede beveiliging investeren zullen de risico's op een datalek kunnen verkleinen, zoals hiervoor ook reeds is vermeld. Al met al verwacht ik dat de meldplicht, en de vertaling ervan naar de praktijk, geen problemen zal hoeven opleveren. Ik wijs hier ook op de meldplicht voor inbreuken op persoonsgegevens in de Telecommunicatiewet waarmee de Autoriteit Consument & Markt al drie jaar ervaring heeft opgedaan. Van die ervaringen zal bij de implementatie van de hier voorgestelde meldplicht uiteraard gebruik worden gemaakt.

De leden van de **PvdA**-fractie vragen voorts of de regering de verwachting reëel acht dat organisaties en instellingen als beleidslijn «better safe than sorry» zullen kiezen en vaker dan nodig is datalekken zullen melden. Als dat het geval is zou daar juist de situatie kunnen ontstaan die de regering wil voorkomen, zoals aangegeven in haar reactie op het voorstel van Bits of Freedom, namelijk dat te veel en te vaak overbodig wordt gemeld.
Ik deel de zorg van de aan het woord zijnde leden op dit punt niet. Met een goede implementatie van dit wetsvoorstel binnen bedrijven en organisaties, en richtsnoeren van het Cbp, verwacht ik geen «overcompliance». Ik acht iedere verantwoordelijke in staat om voor de eigen verwerkingen een inschatting te maken van meldingsplichtige en niet-meldingsplichtige datalekken, gelet op de aard van de inbreuk, de aard van de persoonsgegevens, de technische beschermingsmaatregelen en de potentiële nadelige gevolgen voor de persoonlijke levenssfeer van de betrokkenen.

Deze leden hebben voorts gevraagd of de regering kan aangeven of zij het verantwoord vindt dat de interpretatie van de omschrijving wanneer gemeld moet worden bij de verantwoordelijke voor het datalek ligt en niet bij de wetgever. In reactie hierop kan ik aangeven dat de normen van de Wbp zich tot de verantwoordelijke richten. De meldplicht voor datalekken is daarop geen uitzondering. Van meet af aan is gezocht naar een omschrijving die voldoende precies aangeeft welke datalekken onder de meldplicht vallen en welke er buiten vallen. De verantwoordelijke moet immers weten wat er van hem verwacht wordt en ook dat hij niet elk denkbaar datalek hoeft te melden. Voor iedere wettelijke regeling geldt dat deze in de praktijk bij de toepassing ervan, interpretatie behoeft. Bij de meer open geformuleerde bepalingen is deze ruimte groter dan bij gedetailleerde gedragsvoorschriften. Ook de meldplicht voor datalekken behoeft interpretatie. Elke verantwoordelijke moet een beredeneerde afweging maken of een concreet datalek dat hem ter kennis komt onder het bereik van de meldingsplicht valt. Zoals hiervoor al is aangegeven, heb ik er het volste vertrouwen in dat bedrijven en (overheids)organisaties hiertoe in staat zijn.

In ditzelfde kader zouden de leden van de **PvdA**-fractie graag van de regering vernemen of hacken nu wel of niet tot melding moet leiden. In de memorie van toelichting zegt de regering dat het hacken van een ICT-systeem wel in de categorie te melden datalekken valt, maar het hacken uit de zienswijze van Bits of Freedom niet. Kan de regering aangeven hoe dit precies zit?
Graag voldoe ik aan het verzoek van deze leden. In de memorie van toelichting wordt het hacken (inbreken in digitale systemen) als voorbeeld gegeven van een «inbreuk op beveiligingsmaatregelen» waardoor ongeoorloofde toegang tot persoonsgegevens kan worden verkregen, met alle risico's op misbruik of onrechtmatig gebruik van deze gegevens van dien. Gesteld wordt, in zijn algemeenheid, dat er bij hacken al snel aanleiding zal zijn om de meldplicht na te leven. Datzelfde geldt voor het aangifte doen bij de politie, aangezien hacken een strafbaar feit is (artikel 138ab WvSr). Bij het naleven van de meldplicht gaat het naast de aard van het incident vooral om de aard van de buitgemaakte of gelekte gegevens, de technische beschermingsmaatregelen en de mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkene(n). Of er in het concrete geval een melding bij het Cbp en betrokkene(n) moet worden gedaan, is uiteindelijk dan ook – altijd – afhankelijk van de omstandigheden van het geval.
Voor zover de memorie van toelichting een tegenstrijdigheid oproept tussen de visie van de regering en Bits of Freedom, merk ik het volgende op. In paragraaf 3.2.2. van de memorie van toelichting wordt het zoekraken of hacken van de ledenadministratie van een sportvereniging als voorbeeld genoemd van een datalek dat niet snel aanleiding zal geven tot een melding, aangezien de gevolgen van een dergelijk datalek doorgaans beperkt blijven en ook van de leden van een vereniging kan worden gevergd dat zij een zekere mate van risico aanvaarden. In de zienswijze van Bits of Freedom (29 februari 2012) wordt deze passage bekritiseerd omdat daarbij ten onrechte geen rekening wordt gehouden met een combinatie van gegevens (bijvoorbeeld de ledenlijst en de financiële gegevens van de vereniging, zodat een overzicht van betalingsachterstanden kan worden verkregen). Bovendien kan een verenigingslidmaatschap ook bijzondere of anderszins gevoelige persoonsgegevens kan bevatten, zoals het lidmaatschap van een bepaalde patiëntenvereniging. Het lekken van dergelijke gegevens kan wel degelijk ongunstige gevolgen voor de betrokken personen met zich brengen. Als dat het geval is, dan zal de meldplicht moeten worden nageleefd. Ik kan mij in dit opzicht dus geheel bij de zienswijze van Bits of Freedom aansluiten.

De leden van de **PvdA**-fractie merken op dat de meldplicht in de memorie van toelichting als een administratieve verplichting wordt opgevat. Hieruit spreekt volgens deze leden de suggestie dat de regering de beoordeling of gemeld moet worden opvat als een simpele, digitale beoordeling. Zij vragen of dit klopt of dat de regering deze suggestie wenst weg te nemen.
Ten tijde van het opstellen van de huidige Wbp (eind jaren negentig) werden alleen de bepalingen van administratief-juridische aard geschikt bevonden om door middel van een bestuurlijke boete te worden gehandhaafd. In lijn hiermee kan het Cbp op grond van de huidige Wbp de materiële normen alleen met herstelsancties (last onder dwangsom) afdwingen. Voor bijvoorbeeld de administratieve meldplicht van artikel 27 en 28 Wbp inzake voorgenomen verwerkingen bij het Cbp of bij de functionaris voor de gegevensbescherming, kon het Cbp wel een bestuurlijke boete opleggen. In de passage van de memorie van toelichting waar deze leden op doelen wordt mijns inziens ten onrechte de indruk gewekt dat de meldplicht datalekken een administratieve verplichting is. Ik ben met deze leden eens dat de meldplicht geen simpele, digitale verplichting is, maar dat deze als een materiële norm valt te kenschetsen. Voor de materiële (of: open) normen van de Wbp geldt dat

het lex certa-beginsel bijzondere aandacht verdient, omdat deze normen een afweging van belangen vergen die pas in het concrete geval betekenis krijgen (zie o.a. paragraaf 4 van het advies van de Afdeling advisering van de Raad van State) en de overwegingen dienaangaande in het nader rapport en de tweede nota van wijziging (nrs. 9 en 10). Of een datalek aanleiding tot een melding moet zijn, moet aan de hand van de omstandigheden van het concrete geval worden beoordeeld. Ik heb hiervoor, in reactie op vragen van deze leden al aangegeven, welke omstandigheden hierbij een rol spelen.

Hoewel ook bij de behandeling in de Tweede Kamer de «onbepaaldheid» van de wettelijke verplichting voor de burger uitgebreid ter sprake is gekomen, is het voor de leden van de **CDA**-fractie nog niet volstrekt helder hoe deze norm voldoende duidelijk, voorzienbaar en kenbaar zal zijn (lex certa beginsel). Het is immers voor bedrijven en overheden van belang om aan de hand van feiten en omstandigheden van het concrete geval te kunnen beoordelen of een datalek binnen het bereik van de meldingsplicht valt. De voorgestelde oplossing is dat het Cbp door middel van richtsnoeren een nadere verduidelijking zal geven. Deze richtsnoeren (beleidsregels) zouden dan volgens het voorgestelde, bij nota van wijziging ingevoegde, artikel 67 na overleg met de Ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties worden vastgesteld. Deze procedure is op papier duidelijk, maar het blijft voor de burger moeilijk om te weten wanneer er van een relevante inbreuk op een beveiliging sprake is. Het gaat dan niet aan om te volstaan – zoals de regering doet – met een verwijzing naar het feit dat de normstelling in de Wbp nu eenmaal als algemeen-abstract kan worden gekenschetst in verband met de grote diversiteit aan verwerkingen van persoonsgegevens in de private en publieke sector. Bovendien zal hier een groot verschil zijn wanneer een relatief kleine inbreuk plaatsvindt bij een particuliere vereniging of een kleine onderneming dan wel bij een overheidsinstelling als de Belastingdienst of de Sociale Verzekeringsbank. Kortom, een catalogus van richtsnoeren zal wel tot het kennispakket van een overheidsinstantie behoren, maar dit kan van een zzp'er niet zonder meer worden gevraagd. Deze aanpak leidt tot de aanzienlijke kans dat het Cbp uit angst voor formidabele boetes met veel onnodige c.q. onterechte meldingen zal worden geconfronteerd of juist dat de burgers wegens de onduidelijkheid van de normstelling schouderophalend aan «het hele gedoe» zullen voorbijgaan. Gaarne vernemen de aan het woord zijnde leden het standpunt van de regering hieromtrent.

Zoals ik hierboven in antwoorden op de leden van de **PvdA**-fractie al heb aangegeven verwacht ik niet dat raadpleging van een «catalogus aan richtsnoeren» nodig is, om de meldplicht op een goede manier te kunnen naleven. Het gaat erom dat de verantwoordelijken bewust en zorgvuldig met persoonsgegevens van mensen omgaan, deze gegevens goed beveiligen en hun verantwoordelijkheid nemen als zich een incident voordoet waarbij er persoonsgegevens zoekraken of in verkeerde handen vallen. Ook dan hebben zij verplichtingen, tegenover de toezichthouder en tegenover de personen wier gegevens bij het lek zijn betrokken. Ik meen dat dit niet alleen van (grote) overheidsorganisaties als de Belastingdienst of de Sociale Verzekeringsbank kan worden gevergd, maar evenzeer van particuliere verenigingen, kleine ondernemingen of zzp'ers. Zoals ik ook eerder heb opgemerkt, schat ik het risico van «overcompliance» of «ondercompliance» als betrekkelijk klein in.

5. Sanctionering

De leden van de **VVD**-fractie wijzen erop dat in de toelichting op de tweede nota van wijziging wordt gesproken over de figuur van medepleger als bedoeld in de Algemene wet bestuursrecht (hierna: Awb). Dit kan zijn een bewerker in de zin van de Wbp maar ook een feitelijk opdrachtgever of een feitelijk leidinggevende. Deze leden vragen of dit betekent dat bijvoorbeeld een afdelingshoofd of manager die feitelijk verantwoordelijk is voor een bepaalde gegevensverwerking ook een boete opgelegd kan krijgen als bedoeld in het wetsvoorstel.

De medepleger als bedoeld in artikel 5:1, tweede lid, van de Awb, is degene die naast de pleger, de overtreding pleegt. Een door de verantwoordelijke ingeschakelde bewerker zou onder omstandigheden een medepleger kunnen zijn. Bij het medeplegen moet sprake zijn van een voldoende nauwe en bewuste samenwerking bij het begaan van de overtreding, waarbij het aandeel van een medepleger van voldoende gewicht moet zijn (vgl. HR 2 december 2014, ECLI:NL:HR:3474).
Anders dan deze leden menen, gaat het bij medeplegen niet om gedragingen van feitelijk leidinggevenden en feitelijk opdrachtgevers. In de tweede nota van wijziging is allereerst vermeld dat gelet op het bepaalde in artikel 5:1, tweede lid, Awb zowel aan de verantwoordelijke als pleger van een overtreding van de Wbp een boete kan worden opgelegd, als aan de ingeschakelde bewerker indien deze kan worden aangemerkt als medepleger. Vervolgens wordt vermeld dat in verband met de invoering van de vierde tranche Awb in 2009 bij oplegging van een bestuurlijke boete aan een rechtspersoon wegens overtreding van de Wbp daarnaast of in plaats daarvan ook aan de feitelijk leidinggevende of feitelijk opdrachtgever, zoals bedoeld in artikel 51, tweede en derde lid, Wetboek van Strafrecht, een boete kan worden opgelegd.

Het bestraffen van feitelijke opdrachtgevers of feitelijk leidinggevenden is uitsluitend aan de orde in de context van overtredingen die worden begaan door rechtspersonen. Met het oog hierop zijn in artikel 5:1, derde lid, van de Awb, de bovengenoemde bepalingen van het Wetboek van Strafrecht van overeenkomstige toepassing verklaard. Ingevolge deze bepalingen kan een bestraffende sanctie worden opgelegd aan de rechtspersoon en daarnaast of in plaats daarvan ook aan degenen die feitelijk opdracht hebben gegeven tot of feitelijk leiding hebben gegeven aan de verboden gedraging. In de memorie van toelichting bij de vierde tranche Awb is vermeld dat voor de vraag of er sprake is van een feitelijke opdrachtgevers of feitelijk leidinggevenden kan worden aangehaakt bij reeds bestaande strafrechtjurisprudentie (vgl. HR 16 december 1986, NJ 1987, 321 en HR 21 januari 1992, NJ 1992, 414). Sinds de invoering van de vierde tranche Awb in 2009, komt ook de bestuursrechtelijke jurisprudentie inzake bestuurlijke beboeting tot ontwikkeling (vgl. o.a. Rechtbank Rotterdam 24 september 2014, ECLI:NL:RBROT:2014:7808, CBb 3 juni 2014, ECLI:NL:CBB:2014:200, CBb 20 juni 2013 ECLI:NL:CBB:2013:CA3716, CBb 13 januari 2015, ECLI:NL:CBB:2015:5).

Bij een rechtspersoonlijkheid bezittende onderneming is de rechtspersoon de verantwoordelijke in de zin van de Wbp. Aangezien de verantwoordelijke in de zin van de Wbp de drager is van rechten en verplichtingen, ligt het voor de hand dat het Cbp in geval van overtreding door een rechtspersoon (verantwoordelijke) de rechtspersoon daarvoor een bestuurlijke boete oplegt. Dit neemt echter niet weg dat daarnaast of plaats daarvan natuurlijke personen binnen deze rechtspersoon kunnen worden beboet indien zij feitelijk leiding hebben gegeven respectievelijk opdracht hebben gegeven tot het verrichten van de verboden gedraging en hebben nagelaten om maatregelen te treffen ter voorkoming van een verboden

gedraging en daarmee bewust de kans wordt aanvaard dat deze gedraging zal plaatsvinden. Deze natuurlijke personen kunnen bestuurders zijn van de onderneming, maar het kunnen ook andere personen zijn binnen de organisatie. De boete zal in de praktijk eerder worden opgelegd aan de rechtspersoon. Het beboeten van feitelijk leidinggevenden of feitelijke opdrachtgevers brengt immers een zwaardere bewijslast mee omdat de toezichthouder aannemelijk moet maken dat de natuurlijke persoon daadwerkelijk feitelijk leiding heeft gegeven of feitelijk opdracht heeft gegeven tot het verrichten van de verboden gedraging en heeft nagelaten om maatregelen te treffen om de verboden gedraging te voorkomen.

Deze leden vragen zich voorts af, of een feitelijk leidinggevende en een verantwoordelijke in hun arbeidsovereenkomst kunnen vastleggen of anderszins overeenkomen dat in voorkomende gevallen de verantwoordelijke de feitelijke opdrachtgever of feitelijk leidinggevende compenseert ter waarde van de hoogte van de boete. Deze vraag laat zich, bij de huidige stand van de jurisprudentie, niet eenduidig beantwoorden. Artikel 3:40 BW vormt een begrenzing van de contractsvrijheid van partijen.
Artikel 3:40, eerste lid, bepaalt dat een rechtshandeling die door inhoud of strekking in strijd is met de goede zeden of de openbare orde, nietig is. In aanmerking nemend dat de wetgever met een bestuurlijke boete beoogt dat de wetsovertreder die boete ook zelf in zijn eigen vermogen zal voelen (leedtoevoeging), onder meer als prikkel en afschrikking om in volgende aangelegenheden geen overtreding meer te begaan, lijkt het zeer wel voorstelbaar dat een contractuele afspraak als gevolg waarvan de boete wordt gedragen door een ander dan de persoon aan wie die is opgelegd, door de rechter in strijd met de openbare orde ex artikel 3:40 BW wordt geacht. In twee uitspraken van 16 december 2014 van het Gerechtshof 's-Hertogenbosch heeft het Hof ambtshalve overwegingen van die strekking opgenomen, evenwel zonder hierover tot een inhoudelijk oordeel te komen (Gerechtshof 's-Hertogenbosch 16 december 2014, Rechtspraak Arbeidsrecht 2015/34 en 2015/43). Tegelijkertijd is het de vraag of, in de context van de Wbp, categorisch – dus in alle gevallen waarin een norm wordt geschonden en als gevolg daarvan een bestuurlijke boete wordt opgelegd – kan worden gesteld dat een contractuele afspraak als gevolg waarvan de boete wordt gedragen door een ander dan de persoon aan wie die is opgelegd, ontoelaatbaar is. In voorkomende gevallen zal uiteindelijk de rechter hieromtrent duidelijkheid moeten verschaffen.
Naar verwachting zal het in de praktijk overigens niet vaak voorkomen dat bij overtreding van de Wbp een bestuurlijke wordt opgelegd aan een werknemer (de feitelijke opdrachtgever of de feitelijk leidinggevende). Zoals hiervoor al is toegelicht, zal de boete dan eerder worden opgelegd aan de verantwoordelijke (de rechtspersoon c.q. werkgever).

Ten aanzien van de hoogte van de boete als percentage van de omzet (maximaal 10 procent) vragen de leden van de **PvdA**-fractie zich af of het niet in geld maximeren van deze boete niet heel veel ruimte aan het Cbp geeft. En, zo willen deze leden weten, heeft de regering de consequenties van een dergelijke boete voor een bedrijf overwogen? Is de regering bereid een maximumbedrag vast te stellen teneinde onwenselijke consequenties te voorkomen?
Voor rechtspersonen wordt, net als in het strafrecht sinds 1 januari 2015 het geval is, een maximale geldboete mogelijk gemaakt, die boven het maximumbedrag van de zesde geldboetecategorie uitgaat (artikel 23, zevende lid, WvSr). Bedacht moet worden dat bij rechtspersonen de geldboete de enige hoofdstraf is. Verder speelt bij rechtspersonen, naast de ernst van het feit en het profijt, de draagkracht een belangrijke rol bij bepaling van de hoogte van geldboete – door de wetgever – waarmee een

strafbaar feit maximaal kan worden bestraft. Ondernemingen beschikken over een, in verhouding tot natuurlijke personen, grote(re) draagkracht. Omdat de maximaal op te leggen geldboete voldoende afschrikwekkende werking moet hebben, wordt in de strafwetgeving rekening gehouden met de draagkracht van rechtspersonen. In navolging van het Wetboek van Strafrecht bepaalt artikel 66, tweede en vijfde lid (artikel IVb) dat indien dit in het kader van een passende bestraffing nodig is, in plaats van het maximum van de zesde geldboetecategorie, een geldboete kan worden opgelegd van ten hoogste tien procent van de jaaromzet van de rechtspersoon. Ik ben het met deze leden eens dat het procentuele, relatieve boetemaximum het Cbp de nodige ruimte geeft. Die ruimte is nodig, omdat Wbp-overtredingen ook door (zeer) grote internationale ondernemingen kunnen worden begaan. Aan de andere kant moet worden bedacht dat het relatieve boetemaximum ook in preventieve zin van belang is. Een absoluut maximum van € 810.000 zal voor kleine ondernemingen zeker afschrikwekkend werken, maar niet voor (zeer) grote ondernemingen. De regering acht het om die reden niet wenselijk om een absoluut boetemaximum vast te stellen, zoals deze leden vragen. De regering vertrouwt erop dat het Cbp in concrete gevallen naar een bij het concrete feit en bij de schuld en de draagkracht van de dader passende boete zal zoeken, overeenkomstig artikel 5:46, tweede lid, Awb. Tegen het boetebesluit staat bezwaar en beroep bij de bestuursrechter open.

De Afdeling advisering van de Raad van State (hierna: Afdeling) vroeg de regering of het instrument van (bestuurlijke) strafbaarstelling overwogen is. De regering reageerde daarop door te stellen dat dit instrument naast de bestuurlijke boete geen meerwaarde heeft en het systeem zou compliceren. Naar de mening van de aan het woord zijnde leden was de intentie van de Raad van State om te informeren naar de (bestuurlijke) strafbaarstelling in plaats van de bestuurlijke boete, niet ernaast. De leden van de **PvdA**-fractie verzoeken de regering deze vraag alsnog te beantwoorden.
De Afdeling merkte in haar advies over het voorstel op, dat niet werd gemotiveerd waarom, als het gaat om kleinere feiten, niet voor de bestuurlijke strafbeschikking is gekozen. Met de verwijzing naar «kleinere feiten» meende de regering dat de Afdeling een aparte plaats zou willen inruimen voor de bestuurlijke strafbeschikking, naast de bestuurlijke boete voor de zwaardere feiten. De keuze voor de mogelijkheid om voor overtreding van de materiële bepalingen van de Wbp een bestuurlijke boete te kunnen opleggen is echter vooral ingegeven door het systeem van de EU-verordening waarin de onafhankelijke toezichthouder de bevoegdheid krijgt om overtreding van de verordening met een bestuurlijke boete te bestraffen. Het is de vraag of de verordening ruimte zal laten voor de Nederlandse figuur van de bestuurlijke strafbeschikking. Het is niet gezegd dat een door de onafhankelijke toezichthouder (Cbp) op te leggen bestuurlijke strafbeschikking zich verdraagt met de onafhankelijkheid van de toezichthouder. Bestuursorganen die de bevoegdheid hebben om een bestuurlijke strafbeschikking uit te vaardigen, doen dit immers onder toezicht van en volgens richtlijnen vast te stellen door het College van procureurs-generaal (artikel 257b, tweede lid, WvSv).

De Afdeling heeft voorts de vraag opgeworpen of de bestuurlijke boete en niet strafbaarstelling het geëigende punitieve middel is. De leden van de **PvdA**-fractie vragen de regering om de belangrijkste argumenten voor deze principiële keuze kenbaar te maken.
Het voornaamste argument voor deze keuze is de veronderstelde effectiviteit van de bestuurlijke boete, als onderdeel van het (sanctie)instrumentarium van het Cbp. Het Cbp heeft in de afgelopen vijftien jaar de nodige ervaring opgedaan met het toezicht op de naleving en de bestuurlijke handhaving van de Wbp. Daarnaast dwingt feitelijk het

toegroeien naar het systeem van de EU-verordening algemene gegevensbescherming tot een keuze voor bestuursrechtelijke handhaving. Op grond van de verordening wordt de onafhankelijke toezichthouder bevoegd om een bestuurlijke boete op te leggen bij overtreding van de verordening. Tot slot mag niet onvermeld blijven dat de Tweede Kamer met de motie-Recourt c.s. om uitbreiding van de boetebevoegdheid van het Cbp heeft gevraagd (Kamerstukken II 2011/12, 32 761, nr. 40). Zoals in paragraaf 5.5 van de toelichting bij de tweede nota van wijziging is aangegeven bevat het commune strafrecht voldoende aanknopingspunten voor de met opsporing en vervolging belaste instanties om tegen ernstig misbruik van persoonsgegevens op te treden, zoals bij identiteitsfraude.

De Afdeling heeft daarnaast op de mogelijkheid gewezen dat in de op handen zijnde Algemene verordening gegevensbescherming (COM(2012)11) bepaalde feiten wellicht niet in aanmerking komen voor een bestuurlijke boete. Hoewel de leden van de **PvdA**-fractie er begrip voor hebben dat de regering niet op de EU-verordening heeft gewacht voordat zij met eigen voorstellen kwam, zouden zij graag een beoordeling van de regering willen zien van de kans waar de Afdeling op doelt.
De Afdeling heeft in haar advies inderdaad aangegeven dat gelet op de verschillende ontwerpteksten die op het moment van advisering openbaar of bekend waren, de verordening voor bepaalde feiten mogelijk geen bestuurlijke boete mogelijk zou maken. Hoewel ik die kans klein acht – een geharmoniseerd systeem van door de nationale toezichthouders op te leggen bestuurlijke boetes is één van de kernelementen van de verordening – kan niet worden uitgesloten dat de uiteindelijke verordening ruimte zal laten voor andere sancties.

De leden van de **D66**-fractie merken op dat het Cbp, naast de bestuurlijke boete, ook een bindende aanwijzing kan geven. Het Cbp kan deze bindende aanwijzing, gevolgd door een boete, opleggen in een aantal in de Wbp genoemde gevallen, waaraan in dit wetsvoorstel wordt toegevoegd de mogelijkheid tot het geven van een bindende aanwijzing in geval van een vermoeden van inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, aldus de tekst van het voorgestelde artikel 34a. Ik ben het met deze leden eens, voorzover zij de bindende aanwijzing als een tussenstap beschrijven, vooruitlopend op een bestuurlijke boete bij niet-nakoming van de aanwijzing (vgl. het voorgestelde artikel 66, derde en vijfde lid). De bindende aanwijzing is geen zelfstandig instrument, naast de bestuurlijke boete. Voorzover deze leden het oog hebben op de in artikel 34a, zevende lid, geregelde bevoegdheid voor het Cbp om van de verantwoordelijke te verlangen dat deze alsnog een kennisgeving doet aan personen van wie de gegevens zijn gelekt, dan is daarin ook een bindende aanwijzing te lezen (een species van de algemene bepaling van artikel 66, derde lid), waarvoor geldt dat de niet-nakoming ervan met een bestuurlijke boete kan worden bestraft.

Artikel 34a is als algemeen abstracte norm geformuleerd. Vanwege het lex certa beginsel vragen de leden van de **D66**-fractie of de regering voorbeelden kan geven van inbreuken die in het concrete geval zullen vallen onder het toepassingsbereik van genoemd artikel, voorbeelden die betrekking hebben op inbreuken die leiden tot de aanzienlijke kans op ernstige nadelige gevolgen als ook voorbeelden die betrekking hebben op inbreuken die ernstige nadelige gevolgen tot gevolg hebben.
De leden van de **D66**-fractie vragen naar concrete voorbeelden die onder het bereik van de meldplicht vallen. Zoals ik hiervoor al heb aangegeven, in antwoord op vragen van de leden van de **PvdA**-fractie, is de beant-

woording van de vraag of melding noodzakelijk is, altijd afhankelijk van de feitelijke omstandigheden van het geval. Dit neemt echter niet weg, dat er in zijn algemeenheid voorbeelden van datalekken kunnen worden gegeven die in de betreffende context tot melding aanleiding geven. Ik put hiervoor uit Opinie 03/2014 van de Artikel 29-Werkgroep van 25 maart 2014.[2] De voorbeelden die in deze opinie worden beschreven en toegelicht hebben betrekking op diverse sectoren waarbij als leidraad de meldplicht op grond van de e-privacyrichtlijn (artikel 11.3a Telecommunicatie) is toegepast. Bij de voorbeelden 1 t/m 5 heeft de inbreuk nadelige gevolgen. Bij de voorbeelden 6 en 7 is er een aanzienlijke kans op nadelige gevolgen.

1. Vier laptops zijn gestolen bij een gezondheidscentrum voor kinderen. De laptops bevatten gevoelige gegevens over gezondheid en welzijn en andere persoonsgegevens van meer dan 2000 kinderen.
2. Bij een levensverzekeraar waren persoonsgegevens ongeoorloofd ingezien als gevolg van een kwetsbaarheid in een webapplicatie. Van 700 personen konden naam, adres en formulieren met medische gegevens worden ingezien.
3. Een medewerker van een internetprovider heeft zijn login/wachtwoordgegevens aan een derde partij gegeven die daardoor nagenoeg onbeperkt bij alle klantgegevens (meer dan 100.000) kon komen.
4. Een envelop met credit card betalingsgegevens van 800 personen was per ongeluk niet versnipperd, maar in een vuilnisbak gegooid. Een derde persoon haalde de gegevens uit de vuilniscontainer op straat en verstrekte ze aan andere personen.
5. De versleutelde laptop van een financieel adviseur is uit de auto gestolen. Financiële gegevens (hypotheken, salarissen, leningen) van 1000 personen waren betrokken. Hoewel het wachtwoord van de laptop niet gecompromitteerd is, was er geen back-up voorhanden.
6. Op de website van een telefoonbedrijf kunnen klanten inloggen en hun financiële gegevens en belgegevens kunnen inzien. Een derde partij heeft toegang gekregen tot de database met inlognamen en bijbehorende verhaspelde (onleesbaar gemaakte) wachtwoorden. Het is echter mogelijk dat bepaalde wachtwoorden achterhaald kunnen worden.
7. Een internetprovider biedt de gebruikers de mogelijkheid om details van hun account te zien, zoals onder andere historische zoekgegevens en vaak bezochte websites. Door een fout in de website had eenieder via een simpele truc de mogelijkheid om de accounts van andere gebruikers vrijelijk in te zien. Zonder een sluitende logging is hier niet vast te stellen of dat daadwerkelijk is gebeurd en welke gegevens dan zijn geraadpleegd.

De bindende aanwijzing is bedoeld om de vermoedelijke overtreder op het rechte pad te houden en om hem te dwingen de vermoedelijke inbreuk geheel of gedeeltelijk te herstellen. De leden van de **D66**-fractie vragen zich af of hier is voorzien in rechtsbescherming van de vermoedelijke overtreder. Kunnen de beschermingsbepalingen van de Awb onverkort worden toegepast in geval van bezwaar en beroep tegen een bindende aanwijzing?
De bindende aanwijzing is in het wetsvoorstel opgenomen in verband met het open karakter van de materiële normen van de Wbp en de handhaving ervan (mede) door middel van de bestraffende bestuurlijke boete (lex certa-beginsel). Het Cbp kan alleen een bindende aanwijzing opleggen in situaties waarin het een overtreding heeft geconstateerd (zie artikel 1, onderdeel q, Wbp). De bindende aanwijzing is geen bestuurlijke sanctie (vgl. artikel 5:2, tweede lid Awb), maar een op herstel gerichte, corrige-

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

rende maatregel. De bindende aanwijzing wordt bij beschikking in de zin van de Awb opgelegd. Tegen de beschikking staat op de normale wijze bezwaar en beroep op de bestuursrechter open, zo kan ik deze leden antwoorden.

6. Concentratie van taken bij het Cbp

Ten aanzien van de totstandkoming van nadere normstelling nam de regering het advies van de Afdeling over om de Minister van Veiligheid en Justitie te laten instemmen met de richtsnoeren van het Cbp. Echter, de Tweede Kamer was vervolgens van mening dat dit onwenselijk is omdat de rijksoverheid ook onder de wet valt en had een voorkeur voor overleg tussen het Cbp en de Ministers van Veiligheid en Justitie en van Binnenlandse Zaken en Koninkrijksrelaties. Het aangenomen amendement onder volgnummer 22 realiseert deze aanpassing. De Afdeling had nog een tweede mogelijkheid genoemd, namelijk om die nadere invulling bij algemene maatregel van bestuur (hierna: AMvB) te laten plaatsvinden. De leden van de **PvdA**-fractie kunnen zich voorstellen dat dat een goed alternatief zou zijn. Zij zouden dan ook graag van de regering vernemen of het alternatief van de AMvB door de regering alsnog overwogen is en zo ja, wat de argumenten zijn geweest om dit niet aan de Tweede Kamer voor te leggen.

De Afdeling noemde inderdaad twee mogelijkheden in haar advies om betrokkenheid van de voor de wetgeving verantwoordelijke bewindspersonen bij de richtsnoeren van het Cbp in de wet te waarborgen. Naast de goedkeuring van de richtsnoeren noemde de Afdeling een in haar ogen verdergaande optie, om nadere invulling van de materiële normen van de Wbp te laten plaatsvinden bij algemene maatregel van bestuur. Ik heb in het nader rapport aangegeven dat ik niet voor een (aanvullende) delegatiebepaling voel. Artikel 26 van de Wbp bevat reeds een bevoegdheid om voor een bepaalde sector bij algemene maatregel van bestuur nadere regels te stellen inzake de in artikelen 6 tot en met 11 en 13 van de Wbp geregelde verplichtingen. Deze delegatiegrondslag is tot op heden niet benut. Een logische verklaring hiervoor is dat sectorale wetgeving veelal zelf in een grondslag voor gedelegeerde regelgeving voorziet die mede de bescherming van persoonsgegevens omvat (bijvoorbeeld de Jeugdwet, Telecommunicatiewet, Elektriciteitswet 1998, Gaswet, Vreemdelingenwet 2000 en de Wet structuur uitvoeringsorganisatie werk en inkomen). Voor de sector van de gezondheidszorg is overigens een Besluit elektronische gegevensverwerking door zorgaanbieders in voorbereiding, waarvoor de grondslag van artikel 26 Wbp voor het eerst wordt benut.

7. Tot slot

Het Cbp zal, als het onderhavige wetsvoorstel is aangenomen, verder de naam «Autoriteit persoonsgegevens» dragen. Bij de leden van de **CDA**-fractie is de vraag gerezen of deze benaming wel recht doet aan de taken die het Cbp uitoefent. Het lijkt toch juist de beschermingsfunctie te zijn die de kern vormt van het bestaan van dit college. Gaarne een reactie.

Zoals ook bij de behandeling in de Tweede Kamer naar voren kwam is bij de nieuwe naamgeving niet over één nacht ijs gegaan en heeft uiteindelijk ook het Cbp een voorkeur voor de naam «Autoriteit persoonsgegevens». De nieuwe naam legt het accent op persoonsgegevens, zijnde een categorie van gegevens waarvoor wettelijke regels gelden ter bescherming van die gegevens met het oog op de eerbiediging van de persoonlijke levenssfeer van mensen. Dat het element «bescherming» uit

de naam wegvalt, maakt de naam korter en (meer) in lijn met de naam van andere toezichthoudende autoriteiten, zoals bijvoorbeeld de Autoriteit Consument & Markt of de Kansspelautoriteit.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff